

Wireshark 101



Wireshark 101

Jeffrey L Carrell

Network Instructor

jeff.carrell@teachmeipv6.com

<https://github.com/jeffcarrell/Wireshark-101>

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

1



Wireshark 101

- OSI
- Well-known ports
- IP Headers
- Install WireShark
- Sniffing (Promiscuous Mode)
- TCP handshake

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

2

Wireshark 101



Wireshark 101

- Filtering
- UDP, TCP, and ICMP scanning
- Socket connectivity
- Encapsulation
- Man in the Middle attacks discussion

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

3



OSI Model

APPLICATION	Applications Layer: deals with applications protocols or services common to applications protocols
PRESENTATION	Presentation Layer: agree on the form that data will be in
SESSION	Session Layer: sets up and manages coordinated connections between two or more programs
TRANSPORT	Transport Layer: takes end-to-end responsibility for messages
NETWORK	Network Layer: decides what is the next stop the messages must take to reach its destination, this includes translating names to addresses, and building & maintaining routing tables
DATA LINK	Link Layer: takes responsibility for the message reaching the next link correctly
PHYSICAL	Physical Layer: defines how bits are represented and what types of cable and connectors are used

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

4

Wireshark 101



Well-known ports

Protocol	TCP/UDP	Port Number
File Transfer Protocol (FTP)	TCP	20/21
Secure Shell (SSH)	TCP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name System (DNS)	TCP/UDP	53
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68
Trivial File Transfer Protocol (TFTP)	UDP	69
Hypertext Transfer Protocol (HTTP)	TCP	80
Post Office Protocol (POP) version 3	TCP	110
Network Time Protocol (NTP)	UDP	123
NetBIOS	TCP/UDP	137/138/139
Internet Message Access Protocol (IMAP)	TCP	143
Simple Network Management Protocol (SNMP)	TCP/UDP	161/162
Border Gateway Protocol (BGP)	TCP	179
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP	443
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	TCP/UDP	636
FTP over TLS/SSL	TCP	989/990

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

5



IP(v4) header

```
+-----+
|Version| IHL  |Type of Service|          Total Length          |
+-----+-----+-----+-----+
|          Identification          |Flags|      Fragment Offset      |
+-----+-----+-----+-----+
| Time to Live |   Protocol   |          Header Checksum          |
+-----+-----+-----+-----+
|          Source Address          |
+-----+-----+-----+-----+
|          Destination Address     |
+-----+-----+-----+-----+
|          Options                  |      Padding      |
+-----+-----+-----+-----+
```

Example Internet Datagram Header

<https://tools.ietf.org/html/rfc791>

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

6

Wireshark 101



Wireshark

- Install Wireshark
- Wireshark basics
- Wireshark: color rules, display filters, columns, configuration profiles, packet annotation, and capture filters
- Wireshark labs!!!

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

7



Getting Wireshark

https://www.wireshark.org/download.html

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

8

Wireshark 101



Getting Wireshark

Vendor / Platform
Alpine / Alpine Linux
Apple / macOS
Arch Linux / Arch Linux
Canonical / Ubuntu
Debian / Debian GNU/Linux
The FreeBSD Project / FreeBSD
Gentoo Foundation / Gentoo Linux
HP / HP-UX
NetBSD Foundation / NetBSD
Novell / openSUSE, SUSE Linux
Offensive Security / Kali Linux
PCLinuxOS / PCLinuxOS
Red Hat / Fedora
Red Hat / Red Hat Enterprise Linux
Slackware Linux / Slackware
Oracle / Solaris 11

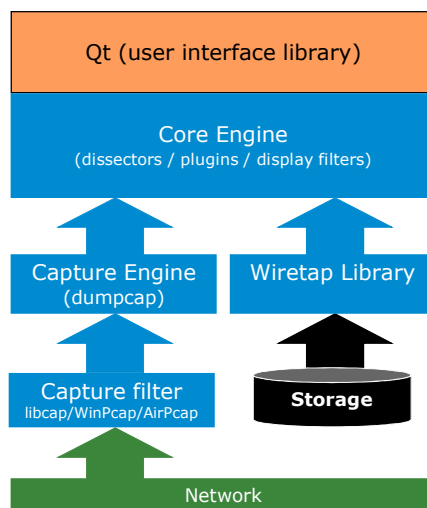
<https://www.wireshark.org/download.html>

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

9



Wireshark operations




- When performing a live capture, you use one of three link layer drivers and go up through the Capture Engine (dumpcap).
- Dumpcap.exe is actually launched to do the capturing – wireshark.exe does not have capture capability.
- When you open a trace file from disk, capture filters cannot be used.
- Wireshark's Wiretap Library can recognize LOTS of trace file formats.
- Dissectors are the powerful elements that pick apart the contents of packets and display their field names and in some cases field interpretations.
- Display filters can be used whether you are performing a live capture or opening a saved trace file.

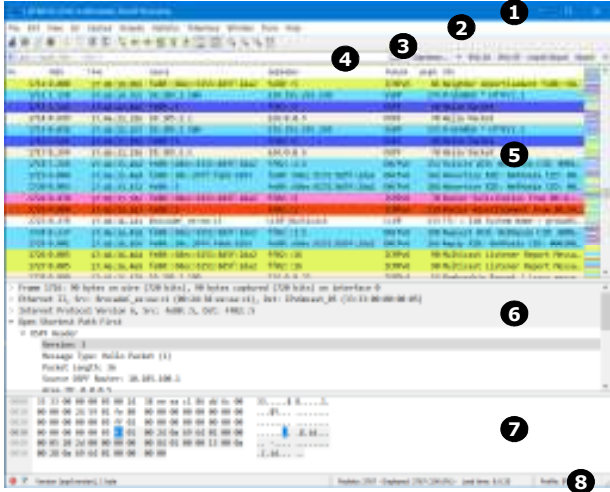
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

10

Wireshark 101




Wireshark main view

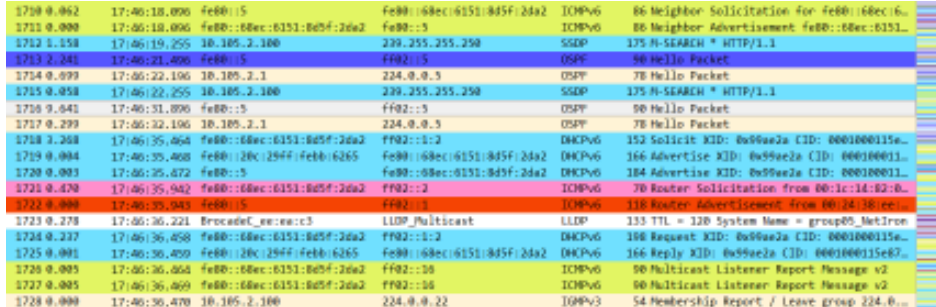


1. Title bar — trace file name or capture device name
2. Main menu — standard menu
3. Main toolbar — quick access
4. Display filter area — reduce the amount of traffic you see
5. Packet List pane — summary of each frame
6. Packet Details pane — dissected frames
7. Packet Bytes pane — hex and ASCII details
8. Status Bar — access to the Expert, annotations, file location, packet counts, and profiles

11



Coloring rules



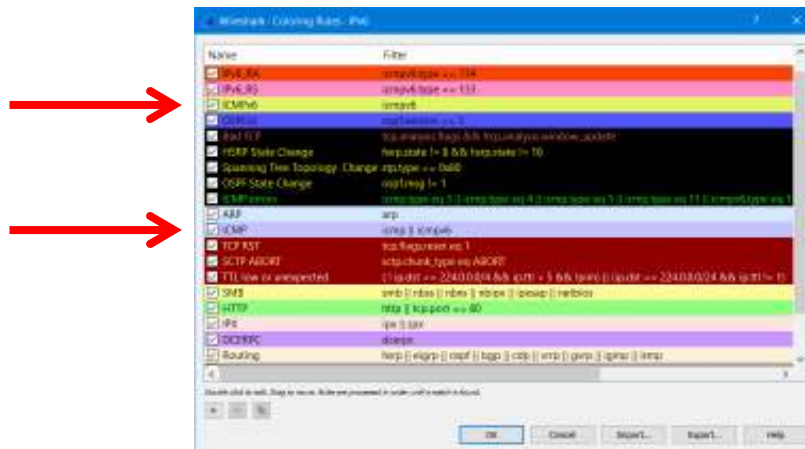
- Colors help you focus on specific address, protocols, events, and possibly find errors quickly

12

Wireshark 101



Color rule processing order



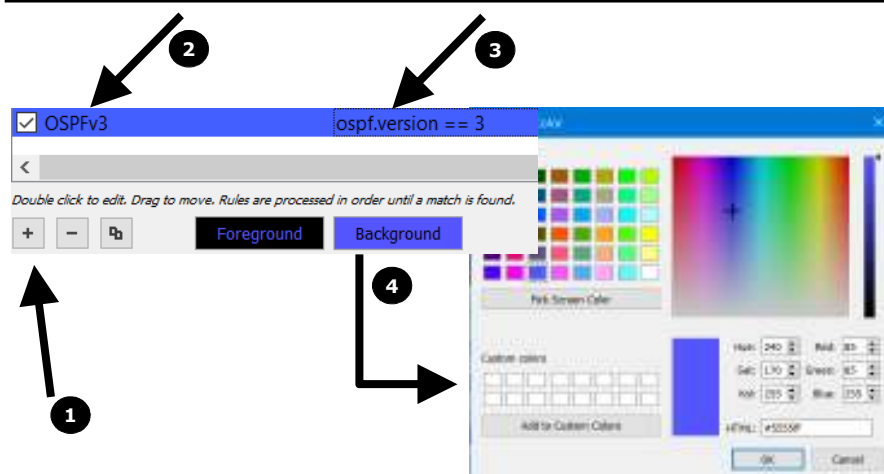
- Color rules read like a router ACL or firewall rules
 - First color rule that matches wins

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

13



Color rule creation



Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

14

Wireshark 101



Display filters – option 1

```
dhcipv6 or icmpv6
ipv6
http.response.code == 200
dhcipv6 or icmpv6.type == 134
ssh
dhcipv6 or icmpv6
(icmpv6.type == 134) || (icmpv6.type == 133)
quic or dns
quic
icmpv6.type == 134
icmpv6.type == 128 or icmpv6.type == 129
```

- The Filter bar will change colors as you type to signify correct syntax for the filter
 - Green – syntax is correct
 - Red – syntax is correct
 - Yellow – syntax is suspect
- The Filter dropdown will show last 10 filters used
- You can save Filter definitions for frequent use

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

15



Display filters – option 2

No.	Time	Source	Destination	Protocol	Length	Info
193	0.000	17:05:16.014	10.105.2.100	224.0.0.252		
194	0.327	17:05:16.942	10.105.2.100	224.0.0.22		
195	0.000	17:05:16.942	17:05:16.942	FF02::1:FF00:107		
196	0.000	17:05:16.942	FE80::680C:6151:805F:2DA2	FF02::16		
197	0.017	17:05:16.959	FE80::680C:6151:805F:2DA2	FF02::16		
198	0.000	17:05:16.959	10.105.2.100	224.0.0.22		
199	0.004	17:05:16.964	FE80::680C:6151:805F:2DA2	FF02::16		
200	0.000	17:05:16.964	10.105.2.100	224.0.0.22		
201	0.001	17:05:16.964	FE80::680C:6151:805F:2DA2	FF02::16		

Frame 195: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: VMware82:04:a3:00:1c:14:82:04:a3, Dst: IPv6cast_FF:00:01:07 (33:33:FF:00:01:07)
Internet Protocol Version 6, Src: ::, Dst: FF02::1:FF00:107
Internet Control Message Protocol v6
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0a3d42 [correct]
[Checksum Status: Good]
Reserved: 00000000
Target Address: 2001:d70:b004:1052::50

Expand Subtree
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy


Shift+Right
Ctrl+Right
Ctrl+Left
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

- In the Packet Details view, right-click on a specific field to build a filter

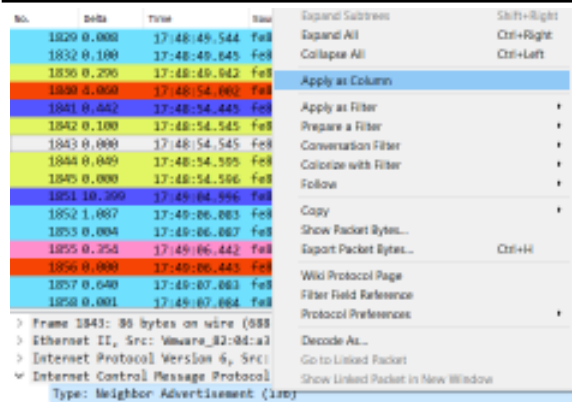
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

16

Wireshark 101



Columns




Source

fe80::68e	Align Left
fe80::5	Align Center
fe80::68e	Align Right
fe80::5	Column Preferences...
fe80::68e	Edit Column
fe80::5	Resize To Contents

- In the Packet Details view, right-click on a specific field to Apply as Column
- Right-click column headings to sort, rename, align, etc

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

17



Configuration profiles

- What they are
- Why/how you use them
- What they contain
- How to share

Default

10162014

AbsDateTime

AbsDateTime and Seq Numbers

Betty-SF15

DFW-CUG

Factory_Default

IP-ID

☒ IPv6

IPv6 Default

IPv6_RA

IPv6_RA_columns

Jeff_main

OpenFlow

Pkt-comments

QOS

RVBD_Wireshark_Workshop_start

RVBD_Wireshark_Workshops

tcpip_4th_v1.0

tcpip_5th_v1.0

TTVN2015

UNT

Wireless


Wireshark-book-review

Wireshark_Workshop

Bluetooth

Classic

Profile: IPv6



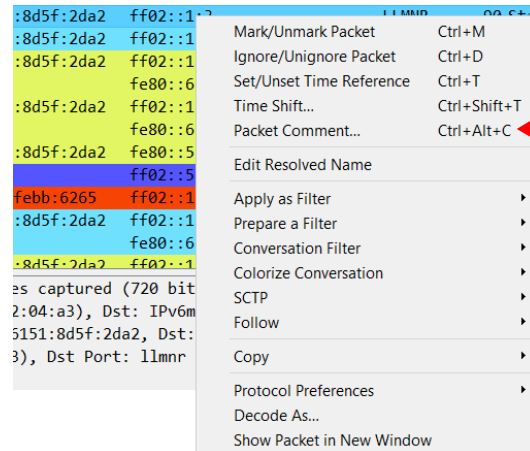
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

18

Wireshark 101



Packet annotation



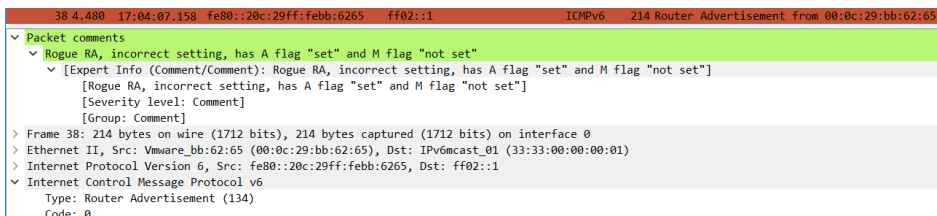
- Right click packet, select Packet Comment

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

19



Packet annotation



Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

20

Wireshark 101

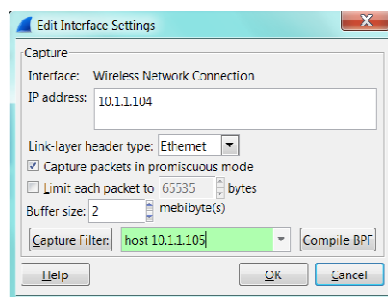


Packet annotation display filter

Wireshark 101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

21

Capture filters



- To configure/apply a capture filter, double-click an adapter in the Capture Options window
- The Capture Filter bar will change colors as you type to signify correct syntax for the filter
 - Green – syntax is correct
 - Red – syntax is correct
 - Yellow – syntax is suspect
- To use a saved capture filter, click the Capture Filter button and select or type in info
- Use capture filters sparingly, as you could inadvertently miss traffic you needed to capture

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

22

Wireshark 101



Capture filters - examples

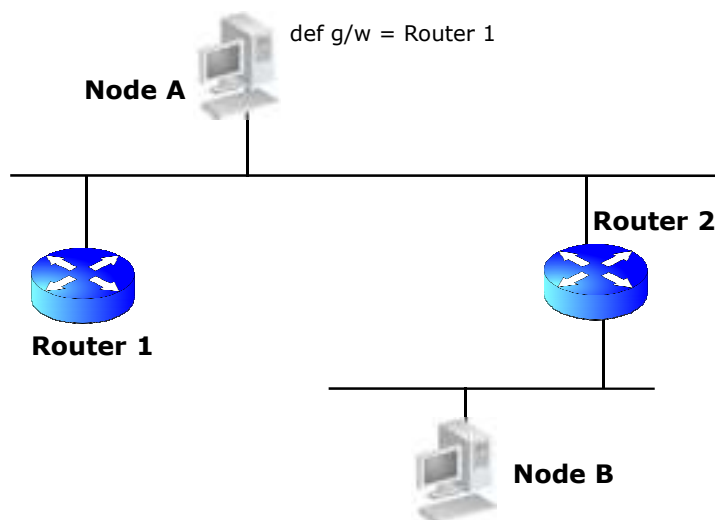
Capture Filter Example	Purpose
ether host 00:08:15:00:08:15	Capture traffic to or from hardware address 00:08:15:00:08:15
host 10.3.1.1	Capture traffic to/from 10.3.1.1
host 2406:da00:ff00::6b16:f02d	Capture traffic to/from the IPv6 address 2406:da00:ff00::6b16:f02d
not host 10.3.1.1	Capture all traffic except traffic to/from 10.3.1.1
src host 10.3.1.1	Capture traffic from 10.3.1.1
host 10.3.1.1 or host 10.3.1.2	Capture traffic to/from 10.3.1.1 and any host it is communicating with and traffic to/from 10.3.1.2 and any host it is communicating with
host www.espn.com	Capture traffic to/from any IP address that resolves to www.espn.com (this will only work if the host name can be resolved by Wireshark prior to capture)
net 10.3.0.0/16	Capture traffic to/from any host on network 10.3.0.0
port 53	Capture UDP/TCP traffic to or from port 53 (typically DNS traffic)
tcp port 21	Capture TCP traffic to or from port 21 (typically the FTP command channel)
portrange 1-80	Capture UDP/TCP traffic to or from ports from 1 through 80
tcp portrange 1-80	Capture TCP traffic to or from ports from 1 through 80
host 10.3.1.1 and port 80	Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1
icmp[0]=8	Capture all ICMP Type 8 (Echo Request) packets.

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

23



Capture – where ?



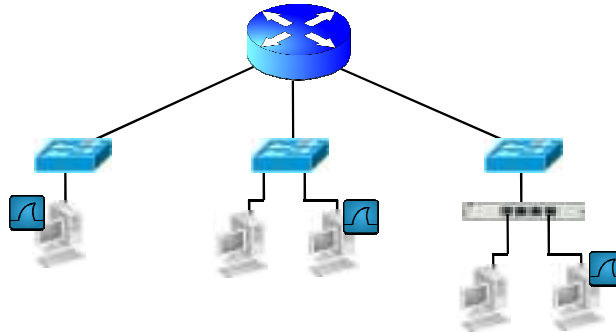
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

24

Wireshark 101



Capture options



- Run Wireshark on the system
- Configure mirror or span port on Layer2/3 switch, run Wireshark on separate device
- Install a "Tap" between system and switch, run Wireshark on separate device

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

25



Top talkers

Conversations: 3 TTVN 2014 Wireshark workshop followme.pcapng

Ethernet II [Hybrid Channel] [UDP] IPv4: 33 [IPv6: 0] [TCP: 3] [UDP: 611] [USB: 0] [WLAN: 0]

Address A	Address B	Packets	Bytes	Packets A -> B	Bytes A -> B	Packets B -> A	Bytes B -> A	Rel. Start	Duration	bps A -> B	bps B -> A
10.1.0.1	10.1.0.200	390	41,956	390	41,956	0	0	48.288013000	947.4001	354.28	N/A
10.1.0.100	10.1.0.200	389	35,942	199	17,649	190	18,293	208.79664/000	790.8881	178.52	185.04
10.1.0.1	10.1.0.100	283	15,571	160	25,248	121	10,121	208.171285000	1160.6552	174.03	71.15
10.1.0.200	192.228.79.201	207	19,639	207	19,639	0	0	55.450252000	940.2380	167.10	N/A
10.1.0.200	192.28.4.12	201	18,486	201	18,486	0	0	55.45067/000	940.2383	157.29	N/A
10.1.0.200	202.12.27.33	187	17,028	187	17,028	0	0	51.272603000	940.3175	144.87	N/A
10.1.0.100	10.1.1.70	119	15,813	119	15,813	0	0	208.370800000	1160.6576	108.98	N/A
10.1.0.200	224.0.0.22	104	6,240	104	6,240	0	0	7.013493000	1335.6708	37.35	N/A
10.1.0.100	229.255.255.250	97	20,245	97	20,245	0	0	108.82526/000	1185.2094	127.33	N/A
10.1.0.100	10.1.0.255	88	11,703	88	11,703	0	0	195.658816000	996.9116	91.91	N/A
10.1.0.100	224.0.0.22	85	5,100	85	5,100	0	0	195.045028000	1172.5672	34.80	N/A
10.1.0.200	224.0.0.252	66	4,480	66	4,480	0	0	7.11677/000	1336.4439	26.82	N/A
10.1.0.200	198.41.0.4	36	5,237	36	5,237	0	0	130.72149000	802.9818	52.18	N/A
10.1.0.100	224.0.0.252	36	2,406	36	2,406	0	0	195.074006000	1172.2107	16.42	N/A
10.1.0.200	10.1.0.255	31	4,003	31	4,003	0	0	9.982023000	912.4713	34.83	N/A
10.1.0.200	192.208.230.10	23	2,137	23	2,137	0	0	128.713816000	795.5122	21.49	N/A

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A-B Graph B-A Close

- Determine top talkers based on MAC addresses, IPv4/IPv6 addresses, port numbers, etc.
- Select: >Statistics >Conversations

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

26

Wireshark 101



Identify applications & protocols

Protocol	% Packets	% Bytes	Packets	Bytes	Transmit	Receive
Ethernet II	100.00%	100.00%	3229	228545	0.00%	0
Internet Protocol Version 6	97.58%	97.58%	2819	204303	0.00%	0
Internet Control Message Protocol v6	5.04%	5.04%	153	12233	0.00%	513
User Datagram Protocol	14.70%	14.70%	440	54518	0.00%	0
Domain Name Service	12.40%	12.40%	389	88887	0.00%	389
DHCPS	1.52%	1.52%	40	2883	0.00%	40
Connectionless Lightweight Directory Access Protocol	0.76%	0.76%	2	441	0.00%	2
Data	0.12%	0.12%	4	4204	0.00%	4
Hypertext Transfer Protocol	0.19%	0.19%	6	1080	0.00%	6
Transmission Control Protocol	0.37%	0.37%	12	1830	0.00%	10
Internet Protocol Version 4	0.00%	0.00%	2004	20723	0.00%	0
Internet Group Management Protocol	0.00%	0.00%	189	11413	0.00%	189
User Datagram Protocol	0.00%	0.00%	1061	108928	0.00%	0
Domain Name Service	0.00%	0.00%	797	63008	0.00%	797
NATOPS Name Service	0.00%	0.00%	12	1266	0.00%	12
NATOPS Datagram Service	0.00%	0.00%	27	6450	0.00%	0
OSPF / OSPFv2 / OSPFv3	0.00%	0.00%	27	6450	0.00%	0

- Identify application and protocols running on the network
- Select: >Statistics >Protocol Hierarchy

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

27



Follow streams

Stream Content:

```
GET / HTTP/1.1
Host: www.ipv6sandbox.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:7.0.1)
Cookie: 20100101; Firefox/7.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
If-Modified-Since: Sat, 03 Mar 2012 20:48:52 GMT
If-None-Match: "/8b9f4a/ff9cc1:0"

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 07 Jun 2012 04:32:48 GMT
Accept-Ranges: bytes
ETag: "48f3ad976644cd1:0"
Server: Microsoft-IIS/7.5
Date: Thu, 10 Oct 2013 04:21:19 GMT
Content-Length: 266

<html>
<head>
<title>ipv6sandbox.com Top page</title>
</head>
```

Online conversation (918 bytes)

Find Save As Print ASCII LUCID Hex Dump C Arrays Raw

Help Filter Out This Stream Close

- Follow Streams
 - TCP
 - UDP
 - SSL
- Select packet (if known 1st in sequence)
- >Analyze > Follow TCP Stream

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

28

Wireshark 101



Wireshark demo – follow me

- Sequence flow
 - watch me on this one
- Open “Wireshark-workshop-follow-jeff.pcapng”
 - Look for these protocols:
 - Telnet
 - SSH
 - HTTP
 - DNS

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

29



Wireshark lab #1

- Open “Wireshark-workshop_lab-file.pcapng”
- Create your own named profile
- Change time/date to time (only) and in milliseconds
- Create/save pkt_comment filter

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

30

Wireshark 101



Wireshark lab #2

- Find 1st pkt with dns.qry.name == "www.ipv6sandbox.com"
 - make a note as to which pkt this is
- Find 1st pkt with DNS query response for www.ipv6sandbox.com
 - make a note as to which pkt this is
 - what is the IP address in the answer section

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

31



Wireshark lab #3

- Find pkt with http.host == "www.ipv6sandbox.com"
 - make a note as to which pkt this is
- Find pkt with an http response code of 200
 - make a note as to which pkt this is
- Find pkt with comment of 'this is the secret pkt with the most important comment!'

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

32

Wireshark 101



Wireshark 101

Questions ???

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

33



Resources


- <https://wiki.wireshark.org/SampleCaptures>
- <https://www.netresec.com/?page=PcapFiles>
- <https://github.com/chrissanders/packets>

- <https://www.cellstream.com/resources/wire-shark-profiles-repository>

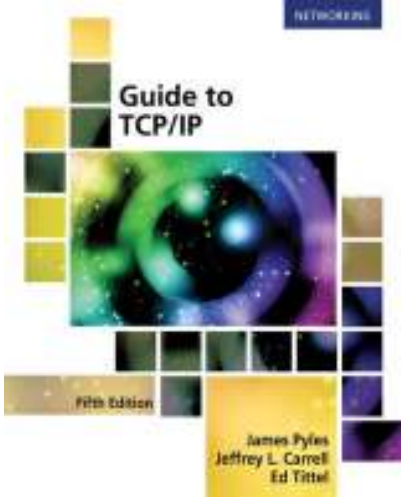
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

34

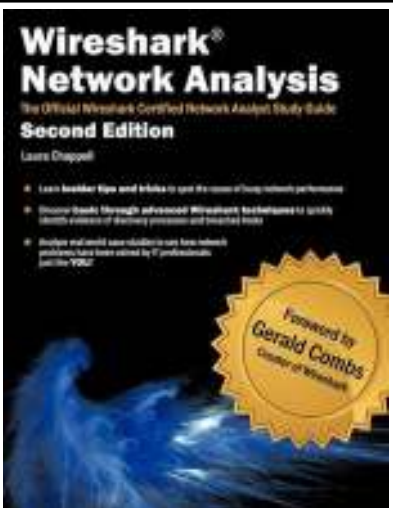
Wireshark 101



Resources



Guide to TCP/IP
Fifth Edition
James Pyles
Jeffrey L. Carrell
Ed Tittel



Wireshark® Network Analysis
The Official Wireshark Certified Network Analyst Study Guide
Second Edition
Laura Chappell

- Learn insider tips and tricks to get the most of Wireshark's performance
- Discover tricks through advanced Wireshark features to quickly identify causes of network problems and resolve them
- Analyze real-world scenarios and how network problems have been solved by IT professionals

Foreword by Gerald Combs
Creator of Wireshark

Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

35



Resources



WIRESHARK
FOR SECURITY PROFESSIONALS
Using Wireshark and the Metasploit Framework
Jesse Bullcock
Joll T. Parker
WILEY



PRACTICAL PACKET ANALYSIS
USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS
CHRIS SANDERS
3RD EDITION

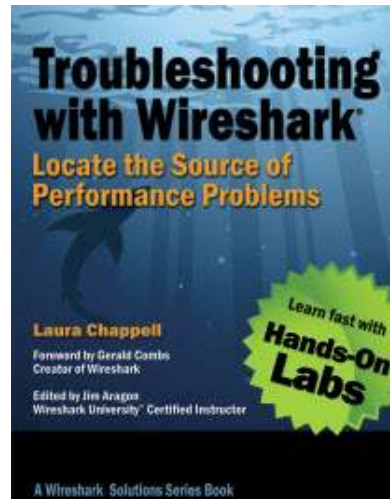
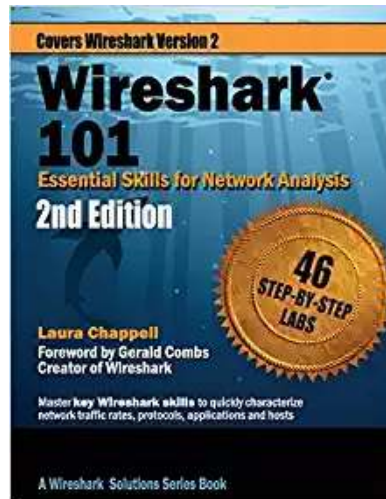
Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

36

Wireshark 101



Resources

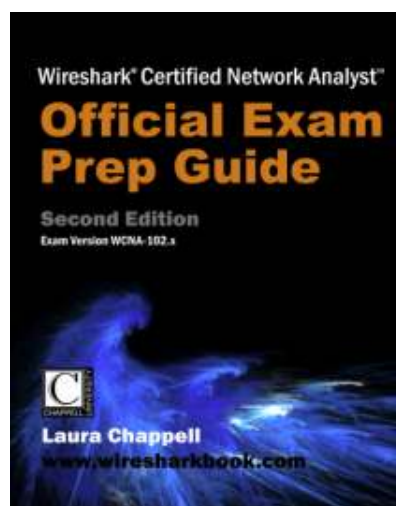


Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

37



Resources



Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

38

Wireshark 101



Thank You for Attending!

- Jeffrey L Carrell
- Network Instructor
- jeff.carrell@teachmeipv6.com



Wireshark-101 v1.0 - Copyright © 2019 Jeffrey L. Carrell

39